

La demostración general

Vamos a extender las ideas utilizadas para $\#KS$ al caso general.

Vale decir, dada una p -relación R auto-reducible, vamos a demostrar que si existe un FPAUG para R , entonces existe un FPRAS para R

Algunos supuestos para la relación R

Suponemos que $R \subseteq \Sigma^* \times \Sigma^*$, y dados $x, w \in \Sigma^*$ definimos:

$$\text{Ext}_R(x, w) = \{y \in \Sigma^* \mid (x, y) \in R \text{ y existe } z \in \Sigma^* \text{ tal que } y = wz\}$$

Algunos supuestos para la relación R

Suponemos que $R \subseteq \Sigma^* \times \Sigma^*$, y dados $x, w \in \Sigma^*$ definimos:

$$\text{Ext}_R(x, w) = \{y \in \Sigma^* \mid (x, y) \in R \text{ y existe } z \in \Sigma^* \text{ tal que } y = wz\}$$

Sean $g : \Sigma^* \rightarrow \mathbb{N}$, $\psi : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ y $\sigma : \Sigma^* \rightarrow \mathbb{N}$ funciones que muestran que R es auto-reducible.

- De acuerdo a la definición vista en las transparencias anteriores

Además, sea $\mathcal{G} : \Sigma^* \times (0, 1) \rightarrow \Sigma^* \cup \{\perp\}$ un FPAUG para R

Algunos supuestos para la relación R

Suponemos que $R \subseteq \Sigma^* \times \Sigma^*$, y dados $x, w \in \Sigma^*$ definimos:

$$\text{Ext}_R(x, w) = \{y \in \Sigma^* \mid (x, y) \in R \text{ y existe } z \in \Sigma^* \text{ tal que } y = wz\}$$

Sean $g : \Sigma^* \rightarrow \mathbb{N}$, $\psi : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ y $\sigma : \Sigma^* \rightarrow \mathbb{N}$ funciones que muestran que R es auto-reducible.

- De acuerdo a la definición vista en las transparencias anteriores

Además, sea $\mathcal{G} : \Sigma^* \times (0, 1) \rightarrow \Sigma^* \cup \{\perp\}$ un FPAUG para R

Finalmente, sean $c, d \in \mathbb{R}^+$ tales que $|\Sigma|^{\sigma(x)} \leq |x|^c + d$ para todo $x \in \Sigma^*$

- Sabemos que existe porque $\sigma(x) \in O(\log(|x|))$

Un esquema de aproximación para R

```
EAR( $x, \varepsilon$ )  
  if  $\mathcal{G}(x, \varepsilon) = \perp$  then return 0  
  else  
     $N := 1$   
     $m := g(x)$   
     $t := \lceil 180 \cdot (|x|^c + d)^3 \cdot m^3 \cdot \varepsilon^{-2} \rceil$   
    while  $g(x) > 0$  do  
      for  $j := 1$  to  $t$  do  
         $y_j := \mathcal{G}\left(x, \frac{\varepsilon}{4m}\right)$   
        Sea  $w \in \Sigma^{\sigma(x)}$  el prefijo de largo  $\sigma(x)$  más común en  $\{y_1, \dots, y_t\}$   
         $\alpha := \frac{|\{j \in \{1, \dots, t\} \mid y_j \in \text{Ext}_R(x, w)\}|}{t}$   
         $x := \psi(x, w)$   
         $N := \frac{1}{\alpha} \cdot N$  /* se tiene que  $\alpha > 0$  */  
  return  $N$ 
```

EAR es un FPRAS para R

Vamos a demostrar que **EAR** es un FPRAS para R

- ▶ Sean $x \in \Sigma^*$ y $\varepsilon \in (0, 1)$ una entrada de **EAR**

EAR es un FPRAS para R

Vamos a demostrar que **EAR** es un FPRAS para R

- ▶ Sean $x \in \Sigma^*$ y $\varepsilon \in (0, 1)$ una entrada de **EAR**

Si $N_R(x) = 0$, tenemos que **EAR**(x, ε) retorna el resultado correcto 0 dado que $\mathcal{G}$ es un FPAUG para R

- ▶ En el resto de la demostración suponemos que $N_R(x) > 0$

EAR es un FPRAS para R

Vamos a demostrar que **EAR** es un FPRAS para R

- ▶ Sean $x \in \Sigma^*$ y $\varepsilon \in (0, 1)$ una entrada de **EAR**

Si $N_R(x) = 0$, tenemos que **EAR**(x, ε) retorna el resultado correcto 0 dado que $\mathcal{G}$ es un FPAUG para R

- ▶ En el resto de la demostración suponemos que $N_R(x) > 0$

De la misma forma, **EAR**(x, ε) retorna el resultado correcto si $g(x) = 0$

- ▶ ¿Por qué?

En el resto de la demostración suponemos que $g(x) > 0$

EAR es un FPRAS para R

Tenemos que el valor de la función g disminuye en cada iteración

- ▶ ¿Por qué?

EAR es un FPRAS para R

Tenemos que el valor de la función g disminuye en cada iteración

- ¿Por qué?

Sea s la cantidad total de iteraciones realizadas por el algoritmo.

- Tenemos que $s \leq g(x) = m$

EAR es un FPRAS para R

EAR funciona en tiempo polinomial en $|x|$ y $\frac{1}{\varepsilon}$

- Puesto que $\mathcal{G}$ es un FPAUG para R , y **EAR** realiza a lo más $m \cdot \lceil 180 \cdot (|x|^c + d)^3 \cdot m^3 \cdot \varepsilon^{-2} \rceil$ llamadas a la función $\mathcal{G}$

EAR es un FPRAS para R

EAR funciona en tiempo polinomial en $|x|$ y $\frac{1}{\varepsilon}$

- Puesto que $\mathcal{G}$ es un FPAUG para R , y **EAR** realiza a lo más $m \cdot \lceil 180 \cdot (|x|^c + d)^3 \cdot m^3 \cdot \varepsilon^{-2} \rceil$ llamadas a la función $\mathcal{G}$

Nos queda entonces por demostrar:

$$\Pr\left(\frac{N_R(x)}{(1 + \varepsilon)} \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x)\right) \geq \frac{3}{4}$$